AO 93 (Rev. 11/13) Search and Seizure Warrant

FILED

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

2018 APR 27 P 12:42

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Samsung Model SM-J700T
S/N R58HB3NFVGL

Case No. 1:18-SW-198

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):

Samsung Model SM-J700T, S/N R58HB3NFVGL, as further described in Attachment A (Property to be Searched).

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B (Property to be Seized).

YOU ARE COMMANDED to execute this warrant on or before April 30, 2018 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to John F. Anderson
(United States Magistrate Judge)

4/27/2018 JFA

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: April 17, 2018 3:15pm

/s/ JFA
John F. Anderson
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

Hon. John F. Anderson, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
1:18-SW-198	4/20-18 1220	Dianne Leucille

Inventory made in the presence of:
Dianne Leveille

Inventory of the property taken and name of any person(s) seized:

Property Samsung SM-S700T Gift with HSC CFA.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 4-20-18

Executing officer's signature

William DeRose, Special Agent

Printed name and title

ATTACHMENT A

The device to be searched includes a Samsung Cellular Phone, Model SM-J700T, Serial Number R58HB3NFVGL.

This warrant authorizes the forensic examination of the devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the devices described in Attachment A which constitute evidence, contraband, or instrumentalities of violations of 31 U.S.C. §§ 5332 including, but not limited to:

a. records regarding potential persons of interest and their related identifying and contact information;

b. records indicating purchased, or otherwise obtained, travel reservations and their related identifying and contact information;

c. text messages regarding the possession, production, sale, provision, and distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

d. records indicating companies or individuals involved in the request for, acquisition of, purchase, sale, manufacturing, storage, transport, receipt, concealment, or distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

e. emails regarding the possession, creation, production, sale, provision and distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

f. notes, photos, videos, or other electronically stored image or document regarding the possession, creation, production, sale, provision, and distribution of falsely made, forged, counterfeited, or altered obligations or other security of the United States and fraudulent money orders;

g. contact lists or phonebooks contained on the devices or in applications accessible on the devices;

h. call lists contained on the devices or in applications accessible on the devices;

i. all calendar entries contained on the devices or in applications accessible on the devices;

j. reminders contained on the devices or in applications accessible on the devices;

k. a list of applications or software loaded onto the devices.

2. Evidence of who used, owned, or controlled the devices at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, phonebooks, photographs, videos, and correspondence.

3. Evidence of the presence or absence of software which would allow others to control the devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the attachment of the devices to other storage devices, phones, or similar containers for electronic evidence;

5. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the devices;

6. Evidence of the times the devices were used;

7. Passwords, encryption keys, and other access devices that may be necessary to access the devices;

8. Documentation and manuals that may be necessary to access the devices or to conduct a forensic examination of the devices;

9. Records of or information about Internet Protocol addresses used by these devices;

10. Records of or information about the devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.